

SOURCE: EnterEdge Technology



May 20, 2008 08:00 ET

InterSOC Enterprise Security Manager Bridges the Gap Between Security Event Data and Policy Compliance

EnterEdge Technology Simplifies Adherence to Regulatory Policies by Translating Security Event Data to Compliance Language

InterSOC website: <http://www.intersoc.com>

ATLANTA, GA--(Marketwire - May 20, 2008) - Regulatory compliance requires companies to have security policies that state they will protect the "confidentiality, privacy, integrity and availability" of their systems, asset data, and customers. According to the security experts at EnterEdge Technology, inventors of the advanced InterSOC solution for total enterprise security management and rapid security threat identification, the challenge is that the event data derived from security, network and system devices isn't delivered in formats that speak this same policy compliance language. As a result, the data produced by typical security solutions offers no solid way to prove or measure performance in terms that match a company's compliance policies.

The average security device produces thousands to millions of events a day and new vulnerabilities are continuously being discovered. The pure volume of data produced by today's complex infrastructure environments -- from IDS, firewalls and system logs to proprietary applications, operating systems, network devices and more -- is often more than can be intelligently monitored or quickly responded to. As such, some companies opt to contract a managed security service to monitor this security data, but often these services do not catch even the most critical security threats. Other companies rely on traditional systems which rate each event based on a "low, medium, high" risk assessment. However, these rankings are often not based on common definitions and don't directly tie back to an organizations' security policy objectives or compliance requirements.

EnterEdge Technology has built a compliance and security threat language into its InterSOC solution by mapping each security event to definitions for policy risk. This allows organizations to configure their security solution by using a combination of policy language and asset knowledge and enables comprehensive reports on security compliance that correlate directly to policy objectives.

"We have developed the InterSOC knowledgebase to maintain and categorize all threat and risk activity using a multidimensional security language that can be easily linked to policy," said Derek John Mezack, senior research scientist, EnterEdge Technology. "This allows users to configure and monitor all policies, monitoring and response activity based on the clear definitions of their compliance policy and gives security and IT administrators the reports they need to effectively communicate security best practices to their executive management."

The InterSOC Enterprise Security Manager bridges the policy gap by delivering comprehensive automated assessment and correlation, liability management, asset health reports, availability monitoring, confidentiality and privacy reporting and trending, misuse detection and automated risk management while integrating data from proprietary systems. This enables organizations to assure client privacy, protect data assets, maintain availability, monitor confidentiality, enforce employee policy, measure asset risks and audit proprietary applications.

"The security of our information system and the privacy of our customers' data is imperative to our business success," said David Turner, CISSP, NSCP Security Administrator, Practiceworks, Inc., Exclusive Maker of Kodak Dental Systems. "InterSOC Enterprise Security Manager automates security management and threat identification so that we can immediately respond to critical threats before users are impacted."

InterSOC's self-updating knowledge base streamlines regulatory compliance requirements while effectively collecting and consolidating security data for real-time modeling of potential security threats through its patent-pending real-time threat modeling architecture. It supports cross-platform and cross-vendor environments including the collection of highly distributed data. By automating the compliance management process, InterSOC ensures adherence to key regulations including PCI, Sarbanes Oxley, HIPAA, FISMA and others.

About EnterEdge Technology and InterSOC

EnterEdge Technology's InterSOC is a sophisticated security management solution that delivers real-time threat modeling that goes beyond data consolidation to provide intelligence on the behavior and attributes of potential security threats before they impact production systems. This real-time Enterprise Security Management (ESM) solution delivers security management, automated threat identification, and incident response capabilities for both packaged and proprietary applications such as those used by healthcare organizations and companies that deliver software as a service. Using an embedded, self-updating knowledge base, InterSOC provides complete visibility and analysis into security threats so that IT administrators can automate compliance management in support of government regulations and corporate governance policies, including "zero-day" threat detection. For more information, please visit: www.intersoc.com.

Contact:
Erin Jones
Carabiner Communications
704.664.2170
ejones@carabinerpr.com